UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

STEVE KLEIN and JOSEPH GERSHON BLIEBERG, Individually and On Behalf of All Others Similarly Situated, Plaintiffs, v. EQUIFAX INC., Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Steve Klein ("Klein") and Joseph Gershon Blieberg ("Blieberg" and, collectively with Klein, "Plaintiffs"), each individually and on behalf of all other persons similarly situated, by their undersigned attorneys, for their complaint against Defendant Equifax Inc. ("Equifax" or the "Company"), allege the following based upon personal knowledge as to themselves and their own acts, and information and belief as to all other matters. Plaintiffs believe that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

INTRODUCTION

1. This is a class action against Equifax for negligence and violations of the Fair Credit Reporting Act ("the FCRA"), 15 U.S.C. §§ 1681 *et seq.* and New York General Business Law ("GBL") Art. 25 §§ 349 and 350, arising out of Defendant's failure to secure the personally identifiable information of Plaintiffs and those similarly situated, including but not limited to names, addresses, birth dates, Social Security numbers, and driver's license numbers, against unauthorized access.

2. Equifax is a global provider of information solutions and human resources business process outsourcing services for businesses, governments, and consumers. The Company is among the largest credit reporting agencies in the United States and collects and aggregates information on over 800 million individuals and 88 million businesses worldwide. The personally identifiable information in Equifax's custody includes social security numbers, birth dates, credit card numbers, driver's license information, and home addresses.

3. Unbeknownst to Plaintiffs and the Class members, however, and contrary to the Company's representations, Equifax's security protocols were inadequate to protect its data systems or to detect data breaches. Beginning in mid-May 2017, a hacker or group of hackers exploited a vulnerability in Equifax website software to gain access, unlawfully, to the private information of as many as 143 million U.S. consumers (the "Data Breach").

4. The vulnerability that enabled the Data Breach to occur existed in Apache Struts, an open-source software framework that Equifax and similar companies use to build websites. This specific vulnerability had been publicly identified in March 2017—two months before the breach—and a patch to fix it, using readily available instructions, had been publicly available since the vulnerability was identified. Accordingly, Equifax new or should have known of the vulnerability as early as March 2017, but did not remedy the vulnerability prior to the Data Breach.

5. Equifax did not discover the Data Breach until July 29, 2017, and then waited an additional 40 days to disclose the breach to the public on the evening of September 7, 2017.

6. Equifax's inadequate security protocols constituted a failure to take adequate and reasonable measures to protect the personal information of Plaintiffs and other Class members from unauthorized access, in intentional, willful, reckless, or negligent disregard of their rights.

7. As a direct consequence of the Data Breach, the personal information of Plaintiffs and other Class members is now subject to criminal misuse by unknown parties, thereby exposing Plaintiffs and other Class members to a number of foreseeable injuries, including both the direct consequences of criminal misuse and the costs entailed in the taking of preventive or ameliorative measures with respect to potential criminal misuse.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) because the aggregate amount in controversy exceeds $5,000,000 and there is diversity between a plaintiff and a defendant.

9. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this Judicial District. Plaintiffs provided information to Defendant, purchased and/or used Defendant's services, and/or purchased credit monitoring services or otherwise undertook preventive or ameliorative measures in response to the Data Breach in this Judicial District.

PARTIES

10. Plaintiff Klein is a natural person residing in Queens, New York. Personal information pertaining to Klein was in the custody of Defendant Equifax as of May 2017, and Klein is a victim of the Data Breach. Klein is a "consumer" within the meaning of 15 U.S.C. § 1681a(c).

11. Plaintiff Blieberg is a natural person residing in Queens, New York. Personal information pertaining to Blieberg was in the custody of Defendant Equifax as of May 2017, and Klein is a victim of the Data Breach. Klein is a "consumer" within the meaning of 15 U.S.C. § 1681a(c).

12. Defendant Equifax is a Delaware corporation with principal executive offices located at 1550 Peachtree Street NE, Atlanta, Georgia 30309. Equifax is authorized to and does conduct business in the State of New York.

13. Defendant Equifax is a "consumer reporting agency" within the meaning of 15 U.S.C. § 1681a(f). Equifax is regularly engaged in the business of assembling, evaluation, and dispersing information concerning consumers for the purpose of furnishing to third parties "consumer reports" within the meaning of 15 U.S.C. § 1681a(d). As such, Equifax's conduct is governed by, and Equifax is subject to the remedies provided by, the FCRA.

SUBSTANTIVE ALLEGATIONS

14. Equifax is headquartered in Atlanta, Georgia and was founded in 1899. Equifax is a global provider of information solutions and human resources business process outsourcing services for businesses, governments, and consumers. It is among the largest credit reporting agencies in the United States.

15. In the course of its business, Equifax aggregates information on over 800 million individuals and 88 million businesses worldwide, including such personally identifiable information as names, addresses, Social Security numbers, birthdates, and driver's license numbers.

16. Having been entrusted with sensitive personally identifiable information, Defendant has a duty to prevent unauthorized access to or disclosure of that information. At all relevant times, Equifax publicly stated, on its website and elsewhere, that it utilized robust data protection protocols to safeguard the personally identifiable information in its custody.

17. In building certain of its website, Equifax utilized an open-source software framework called Apache Struts. In March 2017, the information technology publication Ars

Technica reported an identified vulnerability in Apache Struts. A fix for the bug was quickly made publicly available.

18. Despite the availability of a fix, and despite its duty to prevent unauthorized to or disclosure of the personally identifiable information within its custody, Equifax did not remedy the vulnerability in its website applications.

19. Two months later, in mid-May 2017, a hacker or group of hackers exploited the unaddressed vulnerability in Equifax's website applications in order to gain access to the personally identifiable information of at least 143 million U.S. consumers.

20. It was not until July 29, 2017—some two months later—that Equifax discovered the Data Breach. However, rather than immediately notify consumers of the data breach, Equifax remained silent for more than a month, during which time three Equifax executives sold Company stock holdings worth roughly $1.8 million.

21. Finally, on September 7, 2017, Equifax announced the breach. The Company released a press release, stating, in relevant part:

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

> Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.
>
> "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."
>
> Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection.

22. As a direct result of the Data Breach, Plaintiffs and the Class have been placed at heightened risk of identity theft and financial harm, and/or have been required to incur costs in undertaking mitigating and/or ameliorative measures, such as third party credit repair and monitoring services.

CLASS ACTION ALLEGATIONS

23. Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed nationwide class (the "Class") and New York sub-class (the "Sub-Class") pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2) and/or (b)(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

24. The proposed Class and Sub-Class that Plaintiffs seek to represent are defined as follows:

> **Class:**
>
> All natural persons residing in the United States whose personally identifiable information was subject to unauthorized access in the Data Breach (as defined *supra* at ¶ 3).
>
> **Sub-Class:**
>
> All natural persons residing in the State of New York whose personally identifiable information was subject to unauthorized access in the Data Breach (as defined *supra* at ¶ 3).

25. Excluded from the Class and Sub-Class are: (1) Defendant; any entity or division in which it has a controlling interest; its legal representatives, officers, directors, assignees, and successors; and its current and former employee; and (2) the judicial officers presiding over this matter and members of their immediate families.

26. Plaintiffs reserve the right to amend the Class and Sub-Class definitions and to add additional sub-classes as appropriate if discovery and further investigation reveal that the Class and/or Sub-Class should be expanded, otherwise divided into sub-classes, or modified in any way.

Numerosity & Ascertainability

27. Although the exact number of Class and Sub-Class members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. According to Equifax, the personally identifiable information of at least 143 million U.S. consumers was compromised in the Data Breach. The number of those individuals residing in the State of New York is highly likely to range from several hundred thousand to millions of individuals.

28. The disposition of the claims of the Class and Sub-Class members in a single action will provide substantial benefits to all parties and to the Court. Class and Sub-Class members are readily identifiable by objective means through reasonable effort.

Typicality

29. Plaintiffs' claims are typical of the claims of the Class and Sub-Class members, as Plaintiffs and the other members of the Class and Sub-Class sustained damages arising out of the same wrongful conduct by Defendant, as alleged herein.

Adequate Representation

30. Plaintiffs will fairly and adequately represent and protect the interests of the Class and Sub-Class. Plaintiffs have retained counsel with substantial experience in prosecuting complex and class action litigation nationwide, including consumer class actions.

31. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class and the Sub-Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests adverse to those of the Class or Sub-Class.

Predominance of Common Issues

32. There are numerous questions of law and fact common to Plaintiffs and Class Sub-Class members that predominate over any question affecting only individual Class and Sub-Class members, the answer to which will advance resolution of the litigation as to all Class and Sub-Class members. These common legal and factual issues include, *inter alia*:

a. whether Defendant engaged in the conduct alleged herein;

b. whether Defendant's conduct violates state and/or federal consumer protection statutes;

c. whether Defendant had a duty to safeguard the personally identifiable information of Plaintiffs and the Class and Sub-Class;

d. whether Defendant breached that duty;

e. whether the personally identifiable information of Plaintiffs and the Class and Sub-Class in Defendant's custody was subject to unauthorized access;

f. the appropriate measure of relief; and

g. the extent of the damages caused by Defendant's acts.

Superiority

33. Plaintiffs and other Class and Sub-Class members have all suffered and will continue to suffer harm and damages as a results of Defendant's unlawful and wrongful conduct. A class action is superior to other available means for the fair and efficient adjudication of this controversy.

34. Absent a class action, most Class and Sub-Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class and Sub-Class members' claims, it is likely that few if any Class and Sub-Class members could afford to seek legal redress for Defendant's misconduct as alleged herein. Absent a class action, Class and Sub-Class members will continue to incur damages, and Defendant's misconduct will continue without remedy.

35. Class action treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class action treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

COUNT I

Negligence
(On Behalf of the Class and the Sub-Class)

36. Plaintiffs repeat, reallege, and incorporate by reference each of the foregoing allegations as though fully set forth herein.

37. Defendant owed a duty to Plaintiffs and the other Class and Sub-Class members to safeguard the personally identifiable information in its custody against unauthorized access.

38. Defendant's failure to prevent unauthorized access to that personally identifiable information constituted a breach of its duty to Plaintiffs and the other Class and Sub-Class members.

39. As a direct and proximate result of Defendant's breach, Plaintiffs and the other Class and Sub-Class members were harmed in an amount to be determined at trial.

COUNT II

Willful Violation of the FCRA
(15 U.S.C. §§ 1681b, 1681e, and 1681n)
(On Behalf of the Class and the Sub-Class)

40. Plaintiffs repeat, reallege, and incorporate by reference each of the foregoing allegations as though fully set forth herein.

41. At all relevant times, Plaintiffs and all other Class and Sub-Class members have been "consumers" within the meaning of 15 U.S.C. § 1681a(c).

42. At all relevant times, Defendant has been a "consumer reporting agency" within the meaning of 15 U.S.C. § 1681a(f).

43. In relevant part, 15 U.S.C. § 1681a(f) defines "consumer report" to include:

> any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—
>
> (A) credit or insurance to be used primarily for personal, family, or household purposes;
>
> (B) employment purposes; or
>
> (C) any other purposed authorized under [15 U.S.C. § 1681b].

44. At all relevant times, the personally identifiable information of Plaintiffs and the other Class and Sub-Class members within Defendant's custody, and accessed by third parties as

a consequence of the Data Breach, constituted a "consumer report" with the meaning of 15 U.S.C. § 1681a(d)(1).

45. Pursuant to the FCRA, Defendant, as a consumer reporting agency, is required to "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements" of the FCRA. 15 U.S.C. § 1681(b).

46. Pursuant to the FCRA, Defendant is further required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a). Those purposes are limited to only the following circumstances: (1) in response to a court order; (2) in accordance with the consumer's written instructions; (3) to a person reasonably believe to intend to use the information in connection with credit issuance, employment, insurance underwriting, license eligibility, investment, legitimate business need, or government-issued travel authorization; (4) in response to a government child-support agency request; or (5) in connection with a federal government agency's receivership or liquidation. *See* 15 U.S.C. § 1681b(a)(1)-(6).

47. Defendant did not adopt and maintain reasonable procedures with regard to confidentiality of consumer information or to limiting the furnishing of consumer report information to the enumerated permissible purposes pursuant to the FCRA.

48. Defendant did not take reasonable and appropriate measures to secure, safeguard and protect the personally identifiable information of Plaintiffs and the other Class and Sub-Class members as required by the FCRA.

49. Defendant's foregoing violations of the FCRA proximately caused the Data Breach, in which the personally identifiable information of Plaintiffs and other Class and Sub-Class members was unlawfully accessed by third parties.

50. Because the specific website application vulnerability that enabled the Data Breach was well publicized prior to the Data Breach, and because a fix for that specific vulnerability was available to Defendant prior to the Data Breach, Defendant's foregoing violations of the FCRA were willful and reckless.

51. As a consequence of Defendant's willful and reckless conduct, unknown third parties were able to gain access to the personally identifiable information of Plaintiffs and the other Class and Sub-Class members, and thus the opportunity to misuse that information for purposes impermissible under the FCRA.

52. Plaintiffs and the other Class and Sub-Class members have been damaged by Defendant's willful and reckless violations of the FCRA.

53. Plaintiffs and the other Class and Sub-Class members are thus entitled to recover "any actual damages sustained . . . as a result of the failure [to comply with the FCRA] or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

54. Plaintiffs and the other Class and Sub-Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2)-(3).

COUNT III

Negligent Violation of the FCRA
(15 U.S.C. §§ 1681b, 1681e, and 1681o)
(On Behalf of the Class and the Sub-Class)

55. Plaintiffs repeat, reallege, and incorporate by reference each of the foregoing allegations as though fully set forth herein.

56. At all relevant times, Plaintiffs and all other Class and Sub-Class members have been "consumers" within the meaning of 15 U.S.C. § 1681a(c).

57. At all relevant times, Defendant has been a "consumer reporting agency" within the meaning of 15 U.S.C. § 1681a(f).

58. In relevant part, 15 U.S.C. § 1681a(f) defines "consumer report" to include:

> any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—
>
> (D) credit or insurance to be used primarily for personal, family, or household purposes;
>
> (E) employment purposes; or
>
> (F) any other purposed authorized under [15 U.S.C. § 1681b].

59. At all relevant times, the personally identifiable information of Plaintiffs and the other Class and Sub-Class members within Defendant's custody, and accessed by third parties as a consequence of the Data Breach, constituted a "consumer report" with the meaning of 15 U.S.C. § 1681a(d)(1).

60. Pursuant to the FCRA, Defendant, as a consumer reporting agency, is required to "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements" of the FCRA. 15 U.S.C. § 1681(b).

61. Pursuant to the FCRA, Defendant is further required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a). Those purposes are limited to only the following

circumstances: (1) in response to a court order; (2) in accordance with the consumer's written instructions; (3) to a person reasonably believe to intend to use the information in connection with credit issuance, employment, insurance underwriting, license eligibility, investment, legitimate business need, or government-issued travel authorization; (4) in response to a government child-support agency request; or (5) in connection with a federal government agency's receivership or liquidation. *See* 15 U.S.C. § 1681b(a)(1)-(6).

62. Defendant did not adopt and maintain reasonable procedures with regard to confidentiality of consumer information or to limiting the furnishing of consumer report information to the enumerated permissible purposes pursuant to the FCRA.

63. Defendant did not take reasonable and appropriate measures to secure, safeguard and protect the personally identifiable information of Plaintiffs and the other Class and Sub-Class members as required by the FCRA.

64. Defendant's foregoing violations of the FCRA proximately caused the Data Breach, in which the personally identifiable information of Plaintiffs and other Class and Sub-Class members was unlawfully accessed by third parties.

65. Because the specific website application vulnerability that enabled the Data Breach was well publicized prior to the Data Breach, and because a fix for that specific vulnerability was available to Defendant prior to the Data Breach, Defendant's foregoing violations of the FCRA were at least negligent.

66. Plaintiffs and the other Class and Sub-Class members have been damaged by Defendant's negligent violations of the FCRA.

67. Plaintiffs and the other Class and Sub-Class members are thus entitled to recover "any actual damages sustained." 15 U.S.C. § 1681o(a)(1).

68. Plaintiffs and the other Class and Sub-Class members are also entitled to recover their costs of the action and reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT IV

Violation of GBL §§ 349 and 350
(On Behalf of the Sub-Class)

69. Plaintiffs repeat, reallege, and incorporate by reference each of the foregoing allegations as though fully set forth herein.

70. Plaintiffs and other members of the Sub-Class are "consumers" within the meaning of GBL § 349.

71. Defendant's statements concerning its data protection measures were advertisements within the meaning of GBL § 350.

72. At all relevant times, Defendant has engaged in trade and commerce in New York within the meaning of GBL § 349.

73. In violation of GBL §§ 349 and 350, Defendant's representations that it was safeguarding and would continue to safeguard the personally identifiable information of Plaintiff and the other Class and Sub-Class members were misleading.

74. Plaintiffs and the other Class and Sub-Class members were damaged as a direct and proximate result of Defendant's violations of GBL §§ 349 and 350, in an amount to be proven at trial and/or are entitled to statutory damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs demand judgment against Defendant as follows:

A. Determining that the instant action may be maintained as a class action under Federal Rule of Civil Procedure 23, and certifying Plaintiffs as Class Representatives;

B. Awarding Plaintiffs and the other members of the Class statutory, treble, punitive, or any other form of damages provided by and pursuant to the statutes cited above;

C. Awarding Plaintiffs and the other members of the Class restitution, disgorgement or other monetary or equitable relief provided by and pursuant to the common law claims and statutes cited above or as the Court deems just and proper;

D. Awarding Plaintiffs and the other members of the Class pre-judgment and post-judgment interest;

E. Awarding Plaintiffs and the other members of the Class reasonable attorneys' fees and costs of suit, including expert witness fees; and

F. Awarding such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands trial by jury.

Dated: September 19, 2017

Respectfully submitted,

POMERANTZ LLP

Jeremy A. Lieberman
J. Alexander Hood II
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8655
jalieberman@pomlaw.com
ahood@pomlaw.com

POMERANTZ LLP
Patrick V. Dahlstrom
10 South La Salle Street, Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
Facsimile: (312) 377-1184

Counsel for Plaintiffs